CLAIMS

What is claimed as new and desired to be protected by Letters Patent of the United States is:

1. A method for message authentication, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy to handle the verified digitally signed message for the recipient.

2. The method of Claim 1, wherein employing at least one policy, further comprises employing an unverified policy to handle each message for the recipient that originates from a sender's domain that is unverifiable, wherein the unverified policy enables at least one action including partial rejection, and complete rejection.

3. The method of Claim 1, wherein employing at least one policy, further comprises employing a verified policy to handle each verified digitally signed message for the recipient that originates from the verified domain of the sender, wherein the verified policy enables at least one action including complete acceptance, complete rejection, preferential acceptance, partial rejection, and partial acceptance.

4. The method of Claim 1, wherein employing at least one policy, further comprises employing a system policy to handle each verified digitally signed message for each recipient in

a message system, wherein the system policy enables at least one action for each recipient in the message system including complete acceptance, complete rejection, preferential acceptance, partial acceptance, and partial rejection.

5. The method of Claim 1, wherein employing at least one policy, further comprises employing a user policy for a particular recipient to handle the verified digitally signed message, wherein the user policy enables at least one action for the particular recipient including complete acceptance, complete rejection, preferential acceptance, partial acceptance, and partial rejection.

6. The method of Claim 1, wherein employing at least one policy, further comprises employing a third party to provide a score for a particular domain to a message system for determining a score policy on handling each verified digitally signed message that originates from the scored domain, wherein the score policy enables at least one action including complete acceptance, complete rejection, preferential acceptance, partial acceptance, and partial rejection.

7. The method of Claim 6, wherein the third party aggregates information from at least one recipient in a plurality of message systems for determining the score for the domain.

8. The method of Claim 6, further comprising enabling the third party to provide a suggested score policy for handling each verified digitally signed message from the scored domain based at least in part on the aggregated information, wherein the suggested scored policy enables at least one action including complete acceptance, complete rejection, preferential acceptance, partial acceptance, and partial rejection.

9. The method of Claim 1, wherein employing at least one policy, further comprises employing a statistics policy based on at least one statistic regarding a plurality of verified digitally signed messages that have previously originated from the verified domain, wherein the statistics policy enables the handling of each message that originates from the previously verified domain, and wherein the statistics policy enables at least one action including complete acceptance, complete rejection, preferential acceptance, partial acceptance, and partial rejection.

10. The method of Claim 9, further comprising determining a trend for messaging behavior in regard to a plurality of messages originating from the domain over a period of time.

11. The method of Claim 10, if the trend is determined to represent negative messaging behavior for the domain, employing at least a length of the trend to enable a change in at least one policy associated with the handling of verified digitally signed message for the recipient.

12. The method of Claim 10, if the trend is determined to represent positive messaging behavior for the domain, employing at least a length of the trend to enable a change in at least one policy associated with the handling of verified digitally signed message for the recipient.

13. The method of Claim 1, further comprising displaying a positive visual indication of at least one action, including complete acceptance, preferential acceptance, and partial acceptance of the verified digitally signed message, wherein the positive indication includes at least one of text, graphic, picture, and color.

14. The method of Claim 1, further comprising displaying a negative visual indication of at least one action, including complete rejection, and partial rejection of the verified digitally signed message wherein the negative indication includes at least one of text, graphic, picture, and color.

15. The method of Claim 1, further comprising automatically segmenting an inbox to at least temporarily store each verified digitally signed message in accordance with the at least one policy that enables at least one action, including complete rejection, complete acceptance, preferred acceptance, partial rejection, and partial acceptance.

16. The method of Claim 1, wherein employing at least one policy, further comprises if it is determined that the domain is relatively new to a messaging system, employing a new domain policy for handling an amount of verified digitally signed messages that are less than a

predetermined limit over a period of time, wherein each message less than the predetermined limit is handled with at least partial acceptance.

17. The method of Claim 1, wherein employing the policy, further comprises if it is determined that the domain is relatively new to a messaging system, employing a new domain policy for handling an amount of verified digitally signed messages that are less than a predetermined limit over a period of time, wherein each message that is greater than the predetermined limit is handled with at most partial rejection.

18. The method of Claim 1, further comprising

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

19. The method of Claim 18, wherein the personal digital certificate is associated with an address of the sender.

20. A server for message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy to handle the verified digitally signed message for the recipient.

21. The server of Claim 20, wherein the at least one policy includes at least one of an unverified domain policy, a verified domain policy, a new domain policy, a system policy, a user policy, a statistics policy, and a third party policy.

22. The server of Claim 20, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

23. A client for message authentication, comprising:

a memory for storing instructions;

a processor for enabling actions based on the stored instructions, including:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy to handle the verified digitally signed message for the recipient.

24. The client of Claim 23, wherein the at least one policy includes at least one of an unverified domain policy, a verified domain policy, a new domain policy, a system policy, a user policy, a statistics policy, and a third party policy.

25. The client of Claim 23, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

26. A carrier wave signal that includes instructions for performing actions, comprising:

generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

if a message originates from a sender's address associated with the domain, employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message; and

if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address, employing at least one policy to handle the verified digitally signed message for the recipient.

27. The carrier wave signal of Claim 26, the actions further comprising:

generating a personal digital certificate for the sender based on the public component and the private component of the key pair associated with the domain, wherein the personal digital certificate is associated with an address of the sender;

providing a public component of the personal digital certificate to the recipient along with the verified digitally signed message; and

enabling the recipient to subsequently provide a response message to the sender that is automatically encrypted with the public component of the sender's personal digital certificate.

28. An apparatus for message authentication, comprising:

a means for generating a key pair associated with a domain, wherein a public component of the key pair is accessible to a domain name system (DNS) server that is associated with the domain;

a means for employing a private component of the key pair to digitally sign the message and forwarding the digitally signed message towards a recipient of the message if a message originates from a sender's address associated with the domain; and

a means for employing at least one policy to handle the verified digitally signed message for the recipient if the public component stored with the DNS server verifies that the digitally signed message originated from the domain associated with the sender's address.